Claims

[c1] A method for pairing a first element and a second element, the first element and the second element forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the method comprising:

selecting a first key, the first key being unique in the broadcasting network;

determining a second key according to the first key, such that a combination of the first key and the second key enables to decrypt broadcasted encrypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system;

assigning respectively the first key and the second key to the first element and the second element.

[c2] The method according to claim 1, wherein the control data enables to descramble the scrambled audiovisual information, the method further comprising:

receiving at the first decoding system the encrypted control data;

using the first key at the first element and using the second key at the second element to decrypt the encrypted control data.

[c3] The method according to any one of claims 1 to 2, wherein th e control data is a control word, the audiovisual information being scrambled using the control word.

[c4] The method according to any one of claims 1 to 2, wherein the control data is an Entitlement Control Message (ECM) comprising a control word, the audiovi sual information being scrambled using the control word.

[c5] The method according to any one of claims 1 to 2, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

[c6] The method according to any one of claims 1 to 2, wherein the control data is an Entitlement Management Message (EMM) comprising an exploitation key enabling to decode a control word, the audiovisual information being scrambled using the control word.

[c7] The method according to any one of claims 1 to 6, wherein the encrypted control data is decrypted using a RSA algorithm, the method further comprising:

selecting a first prime number p and a second prime number q;

calculating a modulus number n as being equal to a product of the first prime number p and the second prime number q;

selecting an encrypting key e as being smaller to the modulus number and as being prime with a function of the first prime number p and the second prime number q;

determine a private key as being equal to an inverse of the encrypting key modulus the function of the first prime number p and the second prime number q;

selecting the first key and the second key such that a product of the first key and the second key equals the private key modulo the function of the first prime number p and the second prime number q;

erasing the first prime number p and the second prime number q.

[c8] The method according to claim 7, further comprising:

receiving at each receiving decoding system a message comprising the encrypted control data;

decrypting the encrypted control data using the first key at the first element and the second key at the second element.

[c9] The method according to any one of claims 1 to 2, wherein the encrypted cont rol data is decrypted using a discrete logarithms algorithm, the method further comprising:

selecting a prime number **q**;

selecting a primitive root of the prime number **g**;

and wherein a product of the first key and the second key equals a private key modulo the prime number.

[c10] The method according to claim 9, further comprising:

receiving at each receiving decoding system a message comprising an encrypted information encrypted with a cession key, the message also comprising the primitive root of the prime numbe r **g** power a random number **k**;

using the first key at the first element and using the second key at the second element to calculate the cession key from the prime number power the random number **k**;

decrypting the encrypted information using the cession key.

[c11] The method according to claim 10, wherein the encrypted information is the scrambled audiovisual information.

[c12] The method according to claim 10, wherein the encrypted information is a control word, the audiovisual information being scrambled using the contro l word.

[c13] The method according to any one of claims 1 to 12, further comprising respectively attributing the first key and the second key at least to a third element and a fourth element, the third element and the fourth element forming a second decoding system distinct from the first decoding system.

[c14] The method according to anyone of claims 1 to 13, wherein

the first element is a decoder;

the second element is a portable security module.

[c15] A first decoding system among a plurality of receiving decoding syste ms in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the first decoding system comprising:

a first element to which is assigned a first key, the first key being unique in the broadcasting network;

a second element to which is assigned a second key, the second key being determined according to the first key such that a combination of the first key and the second key enables to decrypt broadcasted enc rypted control data that is received to be decrypted by each receiving decoding system, the encrypted control data being identical for each receiving decoding system.

[c16] The first decoding system according to claim 15, further comprising:

receiving means to receive the broadcasted encrypted control data;

a pair of decryptions comprising a first decryption and a second decryption respectively located in the first element and the second element, the pair of decryptions enabling to decrypt the broadcasted encrypted control data using the first key and the second key.

[c17] The first decoding system according to any one of claims 15 or 16, wherein the broadcasted encrypted control data is decrypted using a discrete logarithm algorithm.

[c18] The first decoding system according to any one of claims 15 or 16, wherein the broadcasted encrypted control data is decrypted using a RSA algorithm.

[c19] The first decoding system according to any one of claims 15 to 18, wherein the control data is a control word, the audiovisual information be ing scrambled using the control word.

[c20] The first decoding system according to any one of claims 15 to 18, wherein the control data is an exploitation key, the exploitation key enabling to decode a control word, the audiovisual information being scrambled us ing the control word.

[c21] The first decoding system according to any one of claims 15 to 20, wherein:
the first element is a decoder;
the second element is a portable security module.

[c22] An apparatus for pairing a first element and a second element, the first ele ment and the second element forming a first decoding system among a plurality of receiving decoding systems in a broadcasting network, each receiving decoding system being adapted to descramble scrambled audiovisual information received over the broadcasting network, the apparatus comprising:

selecting means to select a first key, the first key being unique in the broadcasting network;

processing means to determine a second key according to the first key such that a combination of the first key and the seco nd key enables to decrypt broadcasted encrypted control data that is received at each receiving decoding system to be decrypted, the encrypted control data being identical for each receiving decoding system;

assigning means to respectively assign the firs t key and the second key to the first element and to the second element.